

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-179592

(43)Date of publication of application : 27.06.2003

(51)Int.Cl.

H04L 9/08

(21)Application number : 2001-378413

(71)Applicant : SONY CORP

(22)Date of filing : 12.12.2001

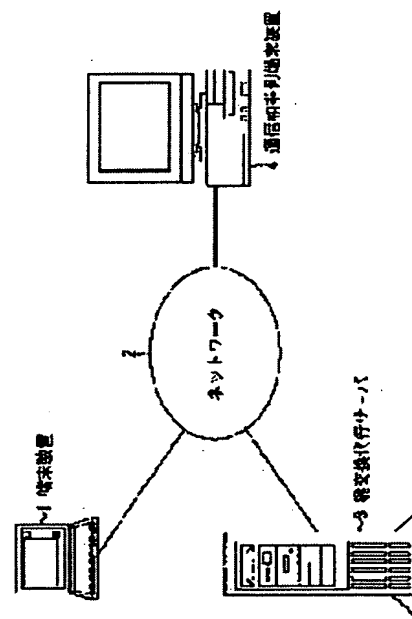
(72)Inventor : HAMANO JUNJI

(54) NETWORK SYSTEM, DEVICE AND METHOD FOR PROCESSING INFORMATION, RECORDING MEDIUM AND PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To reduce a burden caused by key exchange processing in an information processor to perform a communication, and to enable even equipment limited in calculation resources to exchange a key while keeping compatibility with existent key exchange protocol.

SOLUTION: A terminal device 1 is connected to a network 2 representatively such as the Internet and performs the cipher communication of enciphered communication contents with a communicating party terminal device 4 via the network 2 by IPsec, SSL or TLS. A key exchange substitution server 3 is connected to the network and substitutes various kinds of processing such as processing for determining the cipher algorithm or key exchange method of key exchange processing to be performed by the terminal device 1 while using IKE or TLS handshake protocol in order to share a common key with the communication party terminal device 4, key generating processing and authentic processing.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-179592

(P2003-179592A)

(43) 公開日 平成15年6月27日 (2003.6.27)

(51) Int.Cl.⁷

H 0 4 L 9/08

識別記号

F I

H 0 4 L 9/00

テーマコード(参考)

6 0 1 B 5 J 1 0 4

6 0 1 E

6 0 1 C

審査請求 未請求 請求項の数16、OL (全 19 頁)

(21) 出願番号 特願2001-378413(P2001-378413)

(22) 出願日 平成13年12月12日 (2001. 12. 12)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 濱野 淳史

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

Fターム(参考) 5J104 DA03 EA04 EA18 JA03 NA02

NA03 PA07

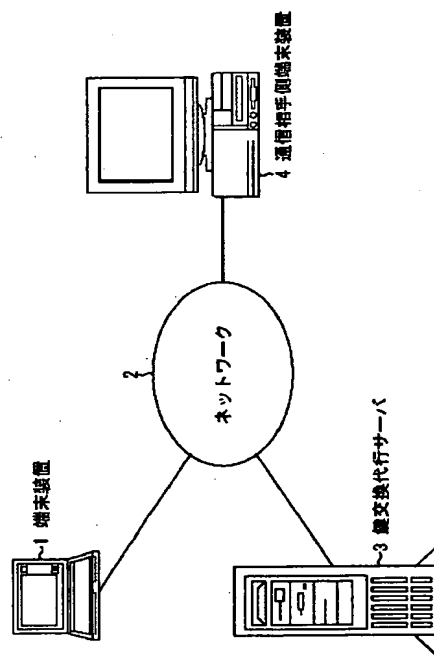
(54) 【発明の名称】 ネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラム

(57) 【要約】

【課題】 通信を行う情報処理装置の鍵交換処理による負担を軽減し、計算資源が限られた機器においても、既存の鍵交換プロトコルとの互換性を保ちつつ鍵交換を実現することができるようにする。

【解決手段】 端末装置1は、インターネット等に代表されるネットワーク2に接続されており、ネットワーク2を介して、IPsec、SSL、またはTSL等により、通信相手側端末装置4と通信内容が暗号化された暗号通信を行う。鍵交換代行サーバ3は、ネットワーク2に接続されており、端末装置1が通信相手側端末装置4と共通鍵を共有するために、IKEやTLS Handshake Protocolを用いて行う鍵交換処理の暗号化アルゴリズムや鍵交換方法を決定する処理、鍵生成処理、および認証処理等の各種処理を代行する。

図1



【特許請求の範囲】

【請求項1】 ネットワークに接続され、他の情報処理装置と暗号通信を行う第1の情報処理装置と、前記ネットワークに接続され、前記第1の情報処理装置が前記暗号通信に用いる共通鍵を、通信相手である前記他の情報処理装置と共有するための、前記第1の情報処理装置による鍵交換処理を代行する第2の情報処理装置とを備えるネットワークシステムであって、前記第1の情報処理装置は、前記他の情報処理装置と前記暗号通信を行う暗号通信手段と、前記鍵交換処理の代行を要求する要求メッセージを前記第2の情報処理装置に供給する要求メッセージ供給手段と、前記要求メッセージ供給手段により供給された前記要求メッセージに対応する応答メッセージを、前記第2の情報処理装置より取得する応答メッセージ取得手段と、前記応答メッセージ取得手段により取得された前記応答メッセージに基づいて、前記暗号通信に用いるセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定手段とを備え、前記第2の情報処理装置は、前記要求メッセージを前記第1の情報処理装置より取得する要求メッセージ取得手段と、前記要求メッセージ取得手段により取得された前記要求メッセージに基づいて、前記鍵交換処理を代行して行う鍵交換代行処理手段と、前記鍵交換代行処理手段の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第1の情報処理装置に供給する応答メッセージ供給手段とを備えることを特徴とするネットワークシステム。

【請求項2】 前記要求メッセージは、前記鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージと、前記共通鍵の生成を要求する鍵生成要求メッセージと、前記第1の情報処理装置の通信相手である前記他の情報処理装置の認証を要求する認証要求メッセージと、前記セッション鍵を要求する鍵要求メッセージとを含み、前記応答メッセージは、前記開始要求メッセージに対応する開始応答メッセージと、前記鍵生成要求メッセージに対応する鍵生成応答メッセージと、前記認証要求メッセージに対応する認証応答メッセージと、前記鍵要求メッセージに対応する鍵応答メッセージとを含み、前記鍵交換代行処理手段は、前記開始要求メッセージに基づいて、前記暗号通信にお

ける鍵交換方法を決定する鍵交換方法決定手段と、前記鍵生成要求メッセージに基づいて、前記共通鍵を生成する共通鍵生成手段と、前記認証要求メッセージに基づいて、前記第1の情報処理装置の通信相手である前記他の情報処理装置を認証する認証手段と、前記認証要求メッセージに基づいて、前記第1の情報処理装置の通信相手である前記他の情報処理装置が前記第1の情報処理装置にアクセス可能か否かを確認する確認手段と、前記鍵要求メッセージに基づいて、前記セッション鍵に関する処理を行うセッション鍵処理手段とを備えることを特徴とする請求項1に記載のネットワークシステム。

【請求項3】 前記鍵交換方法は、IKE、または、SSL若しくはTLSのHandshake Protocolを含むことを特徴とする請求項2に記載のネットワークシステム。

【請求項4】 前記第1の情報処理装置は、前記第2の情報処理装置と安全に通信が行えるか否かを判定する第1の判定手段と、前記第1の判定手段の判定結果に基づいて、前記第2の情報処理装置と安全に通信するための、前記第2の情報処理装置と共有する共通鍵を設定する第1の共通鍵設定手段とをさらに備え、前記第2の情報処理装置は、前記第1の情報処理装置と安全に通信が行えるか否かを判定する第2の判定手段と、前記第2の判定手段の判定結果に基づいて、前記第1の情報処理装置と安全に通信するための、前記第1の情報処理装置と共有する共通鍵を設定する第2の共通鍵設定手段とをさらに備えることを特徴とする請求項1に記載のネットワークシステム。

【請求項5】 ネットワークに接続され、第1の他の情報処理装置と暗号通信を行う情報処理装置であって、前記第1の他の情報処理装置と暗号通信を行う暗号通信手段と、前記暗号通信手段による前記暗号通信に用いる共通鍵を記憶する記憶手段と、前記共通鍵を前記第1の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、前記鍵交換処理を代行する第2の他の情報処理装置に供給する要求メッセージ供給手段と、前記要求メッセージ供給手段により供給された要求メッセージに対応する応答メッセージを、前記第2の他の情報処理装置より取得する応答メッセージ取得手段と、前記応答メッセージ取得手段により取得された前記応答メッセージに基づいて、前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定手段とを備えることを特徴とする情報処理装置。

【請求項6】 前記第2の他の情報処理装置と安全に通信が行えるか否かを判定する判定手段と、

前記判定手段の判定結果に基づいて、前記第2の他の情報処理装置と安全に通信するための、前記第2の他の情報処理装置と共有する共通鍵を設定する共通鍵設定手段とをさらに備えることを特徴とする請求項5に記載の情報処理装置。

【請求項7】 暗号通信に用いる共通鍵を記憶する記憶部を有し、ネットワークに接続され、第1の他の情報処理装置と暗号通信を行う情報処理装置の情報処理方法であって、

前記第1の他の情報処理装置と前記暗号通信を行う暗号通信ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵を前記第1の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、前記鍵交換処理を代行する第2の他の情報処理装置に供給する要求メッセージ供給ステップと、

前記要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、前記第2の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、

前記応答メッセージ取得制御ステップの処理により取得が制御された前記応答メッセージに基づいて、前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特徴とする情報処理方法。

【請求項8】 暗号通信に用いる共通鍵を記憶する記憶部を有し、ネットワークに接続され、第1の他の情報処理装置と前記暗号通信を行う情報処理装置用のプログラムであって、

前記第1の他の情報処理装置と前記暗号通信を行う暗号通信ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵を前記第1の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、前記鍵交換処理を代行する第2の他の情報処理装置に供給する要求メッセージ供給ステップと、

前記要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、前記第2の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、

前記応答メッセージ取得制御ステップの処理により取得が制御された前記応答メッセージに基づいて、前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特

徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項9】 暗号通信に用いる共通鍵を記憶する記憶部を有し、ネットワークに接続され、第1の他の情報処理装置と前記暗号通信を行う情報処理装置を制御するコンピュータが実行可能なプログラムであって、前記第1の他の情報処理装置と前記暗号通信を行う暗号通信ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、

前記暗号通信ステップの処理による前記暗号通信に用いる共通鍵を前記第1の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、前記鍵交換処理を代行する第2の他の情報処理装置に供給する要求メッセージ供給ステップと、

前記要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、前記第2の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、

前記応答メッセージ取得制御ステップの処理により取得が制御された前記応答メッセージに基づいて、前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特徴とするプログラム。

【請求項10】 ネットワークに接続され、第1の他の情報処理装置が、前記第1の他の情報処理装置により行われる暗号通信に用いられる共通鍵を、通信相手である第2の他の情報処理装置と共有するための、前記第1の他の情報処理装置による鍵交換処理を代行する情報処理装置であって、

前記鍵交換処理に関する情報を記憶する記憶手段と、

前記鍵交換処理の代行を要求する要求メッセージを、前記第1の他の情報処理装置より取得する要求メッセージ取得手段と、

前記要求メッセージ取得手段により取得された前記要求メッセージに基づいて、前記鍵交換処理を代行して行う鍵交換代行処理手段と、

前記鍵交換代行処理手段の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第1の他の情報処理装置に供給する応答メッセージ供給手段とを備えることを特徴とする情報処理装置。

【請求項11】 前記要求メッセージは、前記鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージと、

前記共通鍵の生成を要求する鍵生成要求メッセージと、

前記第2の他の情報処理装置の認証を要求する認証要求メッセージと、

前記暗号通信のセッションごとの前記共通鍵であるセッション鍵を要求する鍵要求メッセージとを含み、

前記応答メッセージは、
 前記開始要求メッセージに対応する開始応答メッセージと、
 前記鍵生成要求メッセージに対応する鍵生成応答メッセージと、
 前記認証要求メッセージに対応する認証応答メッセージと、
 前記鍵要求メッセージに対応する鍵応答メッセージとを含み、
 前記鍵交換代行処理手段は、
 前記開始要求メッセージに基づいて、前記暗号通信における鍵交換方法を決定する鍵交換方法決定手段と、
 前記鍵生成要求メッセージに基づいて、前記共通鍵を生成する共通鍵生成手段と、
 前記認証要求メッセージに基づいて、前記第2の他の情報処理装置を認証する認証手段と、
 前記認証要求メッセージに基づいて、前記第2の他の情報処理装置が前記第1の他の情報処理装置にアクセス可能か否かを確認する確認手段と、
 前記鍵要求メッセージに基づいて、前記セッション鍵に関する処理を行うセッション鍵処理手段とを備えることを特徴とする請求項10に記載の情報処理装置。

【請求項12】 前記第2の情報処理装置は、
 前記第1の他の情報処理装置と安全に通信が行えるか否かを判定する判定手段と、
 前記判定手段の判定結果に基づいて、前記第1の他の情報処理装置と安全に通信するための、前記第1の他の情報処理装置と共有する共通鍵を設定する共通鍵設定手段とをさらに備えることを特徴とする請求項10に記載の情報処理装置。

【請求項13】 前記記憶手段により記憶されている前記鍵交換処理に関する情報は、前記第2の他の情報処理装置の認証に関する情報、および前記第2の他の情報処理装置が前記第1の他の情報処理装置にアクセス可能か否かに関する情報であるポリシ情報を含むことを特徴とする請求項10に記載の情報処理装置。

【請求項14】 前記鍵交換処理に関する情報を記憶する記憶部を有し、ネットワークに接続され、第1の他の情報処理装置が、前記第1の他の情報処理装置により行われる暗号通信に用いられる共通鍵を、通信相手である第2の他の情報処理装置と共有するための、前記第1の他の情報処理装置による鍵交換処理を代行する情報処理装置の情報処理方法であって、
 前記鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、
 前記鍵交換処理の代行を要求する要求メッセージの、前記第1の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、
 前記要求メッセージ取得制御ステップの処理により取得が制御された前記要求メッセージに基づいて、前記鍵交換

換処理を代行して行う鍵交換代行処理ステップと、
 前記鍵交換代行処理ステップの処理の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第1の他の情報処理装置に供給する応答メッセージ供給ステップとを備えることを特徴とする情報処理方法。

【請求項15】 前記鍵交換処理に関する情報を記憶する記憶部を有し、ネットワークに接続され、第1の他の情報処理装置が、前記第1の他の情報処理装置により行われる暗号通信に用いられる共通鍵を、通信相手である第2の他の情報処理装置と共有するための、前記第1の他の情報処理装置による鍵交換処理を代行する情報処理装置用のプログラムであって、
 前記鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、
 前記鍵交換処理の代行を要求する要求メッセージの、前記第1の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、
 前記要求メッセージ取得制御ステップの処理により取得が制御された前記要求メッセージに基づいて、前記鍵交換処理を代行して行う鍵交換代行処理ステップと、
 前記鍵交換代行処理ステップの処理の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第1の他の情報処理装置に供給する応答メッセージ供給ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項16】 前記鍵交換処理に関する情報を記憶する記憶部を有し、ネットワークに接続され、第1の他の情報処理装置が、前記第1の他の情報処理装置により行われる暗号通信に用いられる共通鍵を、通信相手である第2の他の情報処理装置と共有するための、前記第1の他の情報処理装置による鍵交換処理を代行する情報処理装置を制御するコンピュータが実行可能なプログラムであって、
 前記鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、
 前記鍵交換処理の代行を要求する要求メッセージの、前記第1の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、
 前記要求メッセージ取得制御ステップの処理により取得が制御された前記要求メッセージに基づいて、前記鍵交換処理を代行して行う鍵交換代行処理ステップと、
 前記鍵交換代行処理ステップの処理の処理結果に基づいて、前記要求メッセージに対応する前記応答メッセージを、前記第1の他の情報処理装置に供給する応答メッセージ供給ステップとを含むことを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、暗号通信における鍵交換処理を代行することにより、通信を行う情報処理装置の負担を軽減するネットワークシステム、情報処理装置および方法、記録媒体、並びにプログラムに関する。

【0002】

【従来の技術】近年、インターネットに代表されるネットワークの普及とともに、電子メールやファイルの送受信がさかんに行われるようになってきた。それに伴い、セキュリティに対する不安も多くなっている。

【0003】従来、インターネット等のネットワークにおいて利用されるセキュリティ機構としては、RFC (Request For Comment) 2401に規定されているIP (Internet Protocol) 層でのセキュリティ機構であるIPsec (Internet Protocol security architecture)、WEBで利用されるSSL (Secure Socket Layer)、および、その後継技術でありRFC2246に規定されているTLS (Transport Layer Security) 等がある。

【0004】これらのプロトコルでは、安全な通信を行う前に、通信者間で暗号通信に利用されるセッション鍵を共有する必要がある。その方法としては、RFC2409で規定されているIKE (Internet Key Exchange)、または、SSLやTLSに含まれるHandshake Protocol等がある。

【0005】IKEは、IPsecに必要な鍵を動的に確立する独立した機構であり、RFC2407およびRFC2408に規定されている、鍵交換の枠組みを提供するISAKMP (Internet Security Association and Key Management Protocol) と、ISAKMP上で実際の鍵管理機構を定義しているOakleyからなる。

【0006】IKEは、ISAKMPのためのISAKMP SA (ISAKMP Security Association) を確立するPhase1と、IPsecのSAを確立するPhase2により構成される。なお、SAとは、通信を保護するために用いられる方針や鍵の集合のことである。Phase1には通信者のIDの保護が可能なメインモードと、IDの保護が不可能なアグレッシブモードの2つが存在し、Phase2にはクイックモードのみが存在する。

【0007】メインモードでは、始動者と応答者の間で、6回(3往復)の通信を行ってISAKMPを確立する。始めの2回(1往復)の通信において両者で使用するアルゴリズム等の取り決めが行われ、次の2回(1往復)の通信において鍵交換に必要なDiffie-Hellman鍵交換アルゴリズムの公開値や乱数等の補助的なデータの交換が行われる。そして、最後の2回(1往復)の通信で生成された鍵の認証が行われる。

【0008】これに対して、アグレッシブモードでは、始動者と応答者の間で、3回(1.5往復)の通信を行い、ISAKMP SAを確立する。始めの2回(1往復)の通

信において両者で使用するアルゴリズム等の取り決めと、鍵交換に必要なDiffie-Hellman鍵交換アルゴリズムの公開値や乱数等の補助的なデータの交換が行われる。そして、3回目の通信において、始動者の認証と生成された鍵の認証が行われる。この3回目の通信は、生成されるISAKMP SAによって暗号化されない。従って、IDの保護が不可能となる。

【0009】メインモード、アグレッシブモードにおいては、電子署名、公開鍵暗号、予め保持している共通鍵を用いる方法の3種類の認証方法が利用可能である。

【0010】Phase2のクイックモードにおいては、始動者と応答者の間で、3回(1.5往復)の通信を行い、IPsecのSAを確立する。クイックモードにおける通信内容は、ISAKMP SAによって保護される。始めの2回(1往復)の通信において、両者で使用するアルゴリズム等の取り決めが行われ、3回目の通信で生成された鍵の認証が行われる。

【0011】以上のようにして、IPsecで安全な通信を行う前に通信者間で暗号通信に利用されるセッション鍵を共有することができる。

【0012】また、TLSは、クライアント-サーバアプリケーションに対してセキュリティを提供するプロトコルであり、鍵交換についてはHandshake Protocolとして規定されている。Handshake Protocolによるクライアント-サーバ間の処理は、以下のように行われる。

【0013】最初に、クライアントは、ClientHelloメッセージを用いて、クライアントで利用可能な暗号化アルゴリズムに関する情報をサーバに供給する。サーバは、その中から使用する暗号化アルゴリズムを選択し、その暗号化アルゴリズムに関する情報を、ServerHelloメッセージを用いてクライアントに供給する。また、サーバは、ServerHelloメッセージを送信した後に、ServerCertificateメッセージを用いてサーバ自身の証明書を送信する。サーバの証明書が存在しない場合、サーバは、合意過程で使用する仮の暗号化鍵等を送信するServerKeyExchangeメッセージをクライアントに送信する。さらに、サーバは、必要であれば、クライアントの証明書の送付を要求するCertificateRequestメッセージも送信する。そして、サーバは、ServerHelloDoneメッセージを送信することによってサーバからの送信を終了し、クライアントからの返答を待つ。

【0014】サーバからCertificateRequestメッセージを送信されたクライアントは、ClientCertificateメッセージによりクライアントの証明書を送信する。そして、証明書を送信したクライアントは、セッション鍵生成の元となるpre-master keyをサーバの公開鍵で暗号化し、その暗号化されたpre-master keyを含むClientKeyExchangeメッセージをサーバに送信する。

【0015】また、クライアントは、ClientHelloメッセージから直前までの通信内容のダイジェストをクライ

アントの秘密鍵で暗号化して、CertificateVerifyメッセージに含めてサーバに送信する。サーバは、それを公開鍵で複合化して、クライアント証明書の正当性を確認する。

【0016】この時点で、セッション鍵などが利用可能となっており、クライアントは、暗号仕様の変更を合図するChangeCipherSpecメッセージを送信した後に、セッション鍵などを設定する。これにより、これ以降の通信は、設定されたセッション鍵を利用して、Helloメッセージで決定したアルゴリズムにより守られるようになる。最後にクライアントは、Finishedメッセージを送信し、終了する。また、サーバにおいても、上述したクライアントの場合と同様に、ChangeCipherSpecメッセージを送信し、セッション鍵などを設定し、Finishedメッセージを送信する。

【0017】以上のようにして、クライアントーサーバ間において、安全な通信を行うためのセッション鍵を共有することができる。

【0018】

【発明が解決しようとする課題】しかしながら、以上のような方法の場合、公開鍵暗号アルゴリズムを利用した認証処理やDiffie-Hellman鍵交換アルゴリズムの計算処理等の負荷の大きな処理が必要であり、計算資源が限られた機器等において、その処理に多大な時間を要する場合があるという課題があった。

【0019】また、特開2001-197055号公報には、機能の乏しい携帯端末であっても、認証局で認証を得た証明書を用いた情報通信を行うことができ、ユーザ等が、複数の認証局が発行した証明書の検証や管理等に対する作業負荷を軽減することが可能な認証代行装置が開示されているが、認証処理の代行のみが目的であり、安全な通信を実現するための鍵の交換方法については提供されていないという課題があった。

【0020】さらに、この場合、ユーザ端末とサーバとの間に認証代行サーバが介在するので、既存の通信プロトコルと互換性を保つことができないという課題もあった。

【0021】本発明はこのような状況に鑑みてなされたものであり、暗号通信における鍵交換処理を代行することにより、通信を行う情報処理装置の負担を軽減することができるようにしたものである。

【0022】

【課題を解決するための手段】本発明のネットワークシステムは、ネットワークに接続され、他の情報処理装置と暗号通信を行う第1の情報処理装置と、ネットワークに接続され、第1の情報処理装置が暗号通信に用いる共通鍵を、通信相手である他の情報処理装置と共有するための、第1の情報処理装置による鍵交換処理を代行する第2の情報処理装置とを備えるネットワークシステムであって、第1の情報処理装置は、他の情報処理装置と暗

号通信を行う暗号通信手段と、鍵交換処理の代行を要求する要求メッセージを第2の情報処理装置に供給する要求メッセージ供給手段と、要求メッセージ供給手段により供給された要求メッセージに対応する応答メッセージを、第2の情報処理装置より取得する応答メッセージ取得手段と、応答メッセージ取得手段により取得された応答メッセージに基づいて、暗号通信に用いるセッションこととの共通鍵であるセッション鍵を設定するセッション鍵設定手段とを備え、第2の情報処理装置は、要求メッセージを第1の情報処理装置より取得する要求メッセージ取得手段と、要求メッセージ取得手段により取得された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理手段と、鍵交換代行処理手段の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第1の情報処理装置に供給する応答メッセージ供給手段とを備えることを特徴とする。

【0023】前記要求メッセージは、鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージと、共通鍵の生成を要求する鍵生成要求メッセージと、第1の情報処理装置の通信相手である他の情報処理装置の認証を要求する認証要求メッセージと、セッション鍵を要求する鍵要求メッセージとを含み、応答メッセージは、開始要求メッセージに対応する開始応答メッセージと、鍵生成要求メッセージに対応する鍵生成応答メッセージと、認証要求メッセージに対応する認証応答メッセージと、鍵要求メッセージに対応する鍵応答メッセージとを含み、鍵交換代行処理手段は、開始要求メッセージに基づいて、暗号通信における鍵交換方法を決定する鍵交換方法決定手段と、鍵生成要求メッセージに基づいて、共通鍵を生成する共通鍵生成手段と、認証要求メッセージに基づいて、第1の情報処理装置の通信相手である他の情報処理装置を認証する認証手段と、認証要求メッセージに基づいて、第1の情報処理装置の通信相手である他の情報処理装置が第1の情報処理装置にアクセス可能か否かを確認する確認手段と、鍵要求メッセージに基づいて、セッション鍵に関する処理を行うセッション鍵処理手段とを備えるようにすることができる。

【0024】前記鍵交換方法は、IKE、または、SSL若しくはTLSのHandshake Protocolを含むようにすることができる。

【0025】前記第1の情報処理装置は、第2の情報処理装置と安全に通信が行えるか否かを判定する第1の判定手段と、第1の判定手段の判定結果に基づいて、第2の情報処理装置と安全に通信するための、第2の情報処理装置と共有する共通鍵を設定する第1の共通鍵設定手段とをさらに備え、第2の情報処理装置は、第1の情報処理装置と安全に通信が行えるか否かを判定する第2の判定手段と、第2の判定手段の判定結果に基づいて、第1の情報処理装置と安全に通信するための、第1の情報処理装置と共有する共通鍵を設定する第2の共通鍵設定

手段とをさらに備えるようにすることができる。

【0026】本発明の第1の情報処理装置は、第1の他の情報処理装置と暗号通信を行う暗号通信手段と、暗号通信手段による暗号通信に用いる共通鍵を記憶する記憶手段と、共通鍵を第1の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、鍵交換処理を代行する第2の他の情報処理装置に供給する要求メッセージ供給手段と、要求メッセージ供給手段により供給された要求メッセージに対応する応答メッセージを、第2の他の情報処理装置より取得する応答メッセージ取得手段と、応答メッセージ取得手段により取得された応答メッセージに基づいて、暗号通信のセッションごとの共通鍵であるセッション鍵を設定するセッション鍵設定手段とを備えることを特徴とする。

【0027】前記第1の情報処理装置は、前記第2の他の情報処理装置と安全に通信が行えるか否かを判定する判定手段と、判定手段の判定結果に基づいて、第2の他の情報処理装置と安全に通信するための、第2の他の情報処理装置と共有する共通鍵を設定する共通鍵設定手段とをさらに備えるようにすることができる。

【0028】本発明の第1の情報処理方法は、第1の他の情報処理装置と暗号通信を行う暗号通信ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵を第1の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、鍵交換処理を代行する第2の他の情報処理装置に供給する要求メッセージ供給ステップと、要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、第2の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、応答メッセージ取得制御ステップの処理により取得が制御された応答メッセージに基づいて、暗号通信のセッションごとの共通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特徴とする。

【0029】本発明の第1の記録媒体のプログラムは、第1の他の情報処理装置と暗号通信を行う暗号通信ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵を第1の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、鍵交換処理を代行する第2の他の情報処理装置に供給する要求メッセージ供給ステップと、要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、第2の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、応答メッセージ取得制御ステップの処理により取得が制御された応答メッセージに基づいて、暗号通信のセッションごとの共

通鍵であるセッション鍵を設定するセッション鍵設定ステップとを含むことを特徴とする。

【0030】本発明の第1のプログラムは、第1の他の情報処理装置と暗号通信を行う暗号通信ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵の記憶部からの取得を制御する記憶制御ステップと、暗号通信ステップの処理による暗号通信に用いる共通鍵を第1の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージを、鍵交換処理を代行する第2の他の情報処理装置に供給する要求メッセージ供給ステップと、要求メッセージ供給ステップの処理により供給された要求メッセージに対応する応答メッセージの、第2の他の情報処理装置からの取得を制御する応答メッセージ取得制御ステップと、応答メッセージ取得制御ステップの処理により取得が制御された応答メッセージに基づいて、暗号通信のセッションごとの共通鍵であるセッション鍵を設定するセッション鍵設定ステップとをコンピュータに実現させる。

【0031】本発明の第2の情報処理装置は、鍵交換処理に関する情報を記憶する記憶手段と、鍵交換処理の代行を要求する要求メッセージを、第1の他の情報処理装置より取得する要求メッセージ取得手段と、要求メッセージ取得手段により取得された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理手段と、鍵交換代行処理手段の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第1の他の情報処理装置に供給する応答メッセージ供給手段とを備えることを特徴とする。

【0032】前記要求メッセージは、鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージと、共通鍵の生成を要求する鍵生成要求メッセージと、第2の他の情報処理装置の認証を要求する認証要求メッセージと、暗号通信のセッションごとの共通鍵であるセッション鍵を要求する鍵要求メッセージとを含み、応答メッセージは、開始要求メッセージに対応する開始応答メッセージと、鍵生成要求メッセージに対応する鍵生成応答メッセージと、認証要求メッセージに対応する認証応答メッセージと、鍵要求メッセージに対応する鍵応答メッセージとを含み、鍵交換代行処理手段は、開始要求メッセージに基づいて、暗号通信における鍵交換方法を決定する鍵交換方法決定手段と、鍵生成要求メッセージに基づいて、共通鍵を生成する共通鍵生成手段と、認証要求メッセージに基づいて、第2の他の情報処理装置を認証する認証手段と、認証要求メッセージに基づいて、第2の他の情報処理装置が第1の他の情報処理装置にアクセス可能か否かを確認する確認手段と、鍵要求メッセージに基づいて、セッション鍵に関する処理を行うセッション鍵処理手段とを備えるようにすることができる。

【0033】前記第2の情報処理装置は、第1の他の情

報処理装置と安全に通信が行えるか否かを判定する判定手段と、判定手段の判定結果に基づいて、第1の他の情報処理装置と安全に通信するための、第1の他の情報処理装置と共有する共通鍵を設定する共通鍵設定手段とをさらに備えるようにすることができる。

【0034】前記記憶手段により記憶されている鍵交換処理に関する情報は、第2の他の情報処理装置の認証に関する情報、および第2の他の情報処理装置が第1の他の情報処理装置にアクセス可能か否かに関する情報であるポリシ情報を含むようにすることができる。

【0035】本発明の第2の情報処理方法は、鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、鍵交換処理の代行を要求する要求メッセージの、第1の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、要求メッセージ取得制御ステップの処理により取得が制御された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理ステップと、鍵交換代行処理ステップの処理の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第1の他の情報処理装置に供給する応答メッセージ供給ステップとを含むことを特徴とする。

【0036】本発明の第2の記録媒体のプログラムは、鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、鍵交換処理の代行を要求する要求メッセージの、第1の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、要求メッセージ取得制御ステップの処理により取得が制御された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理ステップと、鍵交換代行処理ステップの処理の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第1の他の情報処理装置に供給する応答メッセージ供給ステップとを含むことを特徴とする。

【0037】本発明の第2のプログラムは、鍵交換処理に関する情報の記憶部からの取得を制御する記憶制御ステップと、鍵交換処理の代行を要求する要求メッセージの、第1の他の情報処理装置からの取得を制御する要求メッセージ取得制御ステップと、要求メッセージ取得制御ステップの処理により取得が制御された要求メッセージに基づいて、鍵交換処理を代行して行う鍵交換代行処理ステップと、鍵交換代行処理ステップの処理の処理結果に基づいて、要求メッセージに対応する応答メッセージを、第1の他の情報処理装置に供給する応答メッセージ供給ステップとをコンピュータに実現させる。

【0038】本発明のネットワークシステムにおいては、ネットワークに接続され、他の情報処理装置と暗号通信を行う第1の情報処理装置と、ネットワークに接続され、第1の情報処理装置が暗号通信に用いる共通鍵を、通信相手である他の情報処理装置と共有するための、第1の情報処理装置による鍵交換処理を代行する第2の情報処理装置とが備えられ、第1の情報処理装置に

おいては、他の情報処理装置と暗号通信が行われ、鍵交換処理の代行を要求する要求メッセージが第2の情報処理装置に供給され、要求メッセージに対応する応答メッセージが、第2の情報処理装置より取得され、応答メッセージに基づいて、暗号通信に用いるセッションごとの共通鍵であるセッション鍵が設定され、第2の情報処理装置においては、要求メッセージが第1の情報処理装置より取得され、その要求メッセージに基づいて、鍵交換処理が代行して行われ、鍵交換代行処理手段の処理結果に基づいて、要求メッセージに対応する応答メッセージが、第1の情報処理装置に供給される。

【0039】本発明の第1の情報処理装置および方法、並びにプログラムにおいては、第1の他の情報処理装置と暗号通信が行われ、暗号通信に用いる共通鍵が記憶され、共通鍵を第1の他の情報処理装置と共有するための鍵交換処理の代行を要求する要求メッセージが、鍵交換処理を代行する第2の他の情報処理装置に供給され、その要求メッセージに対応する応答メッセージが、第2の他の情報処理装置より取得され、その応答メッセージに基づいて、暗号通信のセッションごとの共通鍵であるセッション鍵が設定される。

【0040】本発明の第2の情報処理装置および方法、並びにプログラムにおいては、鍵交換処理に関する情報が記憶され、鍵交換処理の代行を要求する要求メッセージが、第1の他の情報処理装置より取得され、その要求メッセージに基づいて、鍵交換処理が代行して行われる、鍵交換代行処理手段の処理結果に基づいて、要求メッセージに対応する応答メッセージが、第1の他の情報処理装置に供給される。

【0041】

【発明の実施の形態】図1は、本発明を適用した鍵交換処理代行システムの構成例を表している。

【0042】図1において、端末装置1は、インターネット等に代表されるネットワーク2に接続されており、ネットワーク2を介して、IPsec、SSL、またはTLS等により、通信相手側端末装置4と通信内容が暗号化された暗号通信を行う。鍵交換代行サーバ3は、ネットワーク2に接続されており、端末装置1が通信相手側端末装置4と共通鍵を共有するために行う鍵交換処理の鍵生成処理や認証処理等を代行する。

【0043】なお、図1において、ネットワーク2には、端末装置1、鍵交換代行サーバ3、および通信相手側端末装置4が1台ずつ接続されているが、これに限らず、端末装置1、鍵交換代行サーバ3、および通信相手側端末装置4がそれぞれ複数接続されていてもよい。

【0044】図2は、端末装置1の構成例を示すブロック図である。

【0045】図2において、CPU (Central Processing Unit) 11は、ROM (Read Only Memory) 12に記憶されているプログラム、または記憶部23からRAM (Rando

m Access Memory) 13 にロードされたプログラムに従って各種の処理を実行する。RAM 13 にはまた、CPU 1 が各種の処理を実行する上において必要なデータなども適宜記憶される。CPU 11、ROM 12、および RAM 13 は、バス 14 を介して相互に接続されている。このバス 14 にはまた、入出力インタフェース 20 も接続されている。

【0046】入出力インタフェース 20 には、キーボード、マウスなどよりなる入力部 21、CRT (Cathode Ray Tube)、LCD (Liquid Crystal Display) などよりなるディスプレイ、並びにスピーカなどよりなる出力部 22、ハードディスクなどより構成される記憶部 23、モデム、ターミナルアダプタなどより構成される通信部 24、および、メモリやハードディスク等で構成される暗号鍵データベース 25 が接続されている。通信部 24 は、ネットワーク 2 を介しての通信処理を行う。通信部 24 はまた、他のユーザ端末との間で、アナログ信号またはデジタル信号の通信処理を行う。また、暗号鍵データベース 25 は、鍵交換代行サーバ 3、または通信相手側端末装置 4 との通信の内容を暗号化するための鍵情報を記録している。

【0047】入出力インタフェース 20 にはまた、必要に応じてドライブ 30 が接続され、磁気ディスク 41、光ディスク 42、光磁気ディスク 43、或いは半導体メモリ 44 などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部 23 にインストールされる。

【0048】図 3 は、鍵交換代行サーバ 3 の構成例を示すブロック図である。

【0049】図 3 において、鍵交換代行サーバ 3 は、図 2 の端末装置 1 の CPU 11 乃至通信部 24 に対応する CPU 51 乃至通信部 64 を有しており、その基本的構成は、端末装置 1 と同様であるので、その説明は省略する。

【0050】また、図 3 において、入出力インタフェース 60 は、さらに、データベース 65 を有している。データベース 65 は、端末装置 1 との通信の内容を暗号化するための鍵情報に関する情報、通信相手側端末装置 4 を認証する認証鍵に関する情報、および、端末装置 1 へのアクセスが許可された装置に関する情報等が記憶されている。

【0051】さらに、入出力インタフェース 60 には、必要に応じてドライブ 70 が接続され、磁気ディスク 81、光ディスク 82、光磁気ディスク 83、或いは半導体メモリ 84 などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部 63 にインストールされる。

【0052】なお、図示は省略するが、通信相手側端末装置 4 も、図 2 に示した端末装置 1 と基本的に同様の構成を有するコンピュータにより構成される。

【0053】次に、図 4 および図 5 のフローチャートを

参照して、端末装置 1 による鍵交換代行処理を説明する。また、必要に応じて、図 6 および図 7 を参照して説明する。

【0054】通信相手側端末装置 4 と鍵交換を行う端末装置 1 の CPU 11 は、最初に、ステップ S1 において、鍵交換代行サーバ 3 との間に安全な通信路が確保されるか否かを判定する。

【0055】確保されないと判定した場合、CPU 11 は、ステップ S2 に進み、鍵交換代行サーバ 3 と安全に通信するための鍵を暗号鍵データベース 25 に設定し、ステップ S3 に進む。なお、設定される鍵は、予め決められており、鍵交換代行サーバ 3 と暗号通信ができるように、鍵交換代行サーバ 3 に設定される鍵と対応してある。また、ステップ S1 において、鍵交換代行サーバ 3 との間に安全な通信路が確保されると判定した場合、CPU 11 は、ステップ S3 に進む。

【0056】すなわち、端末装置 1 と鍵交換代行サーバ 3 との間が安全な通信路である場合、両者間の通信は、通常の通信により行われるが、端末装置 1 と鍵交換代行サーバ 3 との間が安全な通信路でない場合は、通信内容を暗号化した暗号通信により行われる。

【0057】図 6 は、端末装置 1 と鍵交換代行サーバ 3 との間が安全な通信路である場合の端末装置 1 の通信に関する主な処理の流れを示す図である。

【0058】図 6 において、安全な通信路を用いて鍵交換代行サーバ 3 に情報を供給する場合、CPU 11 の処理部 101 は、通信部 24 を介して、鍵交換代行サーバ 3 に情報を供給する。また、安全な通信路を用いて鍵交換代行サーバ 3 より情報を取得する場合、CPU 11 の処理部 101 は、通信部 24 を介して、鍵交換代行サーバ 3 より情報を取得する。

【0059】通信相手側端末装置 4 に情報を供給する場合、CPU 11 の処理部 101 は、暗号通信部 102 に情報を供給する。暗号通信部 102 は、暗号鍵データベース 25 より必要な鍵情報を取得し、処理部 101 より供給された情報を暗号化する。情報を暗号化した暗号通信部 102 は、通信部 24 を介して、暗号化した情報を通信相手側端末装置 4 に供給する。また、通信相手側端末装置 4 より情報を取得する場合、供給された情報は、通信部 24 を介して暗号通信部 102 に供給される。暗号通信部 102 は、暗号鍵データベース 25 より必要な鍵情報を取得し、通信部 24 を介して供給された情報を復号し、処理部 101 に供給する。

【0060】すなわち、端末装置 1 は、通信相手側端末装置 4 と暗号通信を行い、鍵交換代行サーバ 3 と暗号化されていない通常の通信を行う。

【0061】また、図 7 は、端末装置 1 と鍵交換代行サーバ 3 との間が安全な通信路でない場合の端末装置 1 の通信に関する主な処理の流れを示す図である。

【0062】図 7 において、鍵交換代行サーバ 3 または

通信相手側端末装置4に情報を供給する場合、CPU11の処理部101は、暗号通信部102に情報を供給し、暗号鍵データベース25より必要な鍵情報を取得させ、供給した情報を暗号化させる。そして、情報を暗号化した暗号通信部102は、通信部24を介して、暗号化した情報を鍵交換代行サーバ3または通信相手側端末装置4に供給する。また、鍵交換代行サーバ3または通信相手側端末装置4より情報を取得する場合、供給された情報は、通信部24を介して暗号通信部102に供給される。暗号通信部102は、暗号鍵データベース25より必要な鍵情報を取得し、通信部24を介して供給された情報を復号し、処理部101に供給する。

【0063】すなわち、端末装置1は、鍵交換代行サーバ3および通信相手側端末装置4のいずれの場合も暗号通信を行う。従って、この場合、ステップS3以降の処理において、端末装置1と鍵交換代行サーバ3の間の通信は、全て暗号化されて行われる。以下の説明において、端末装置1が行う暗号化および復号する処理は図7において説明した場合と同様であるので、その説明は省略する。

【0064】図4に戻り、ステップS3において、CPU11は、鍵交換代行サーバ3に鍵交換処理の開始を示し、鍵交換方法の決定を要求する開始要求メッセージを供給する。開始要求メッセージには、端末装置1において利用可能な暗号化アルゴリズムやハッシュアルゴリズムのリスト等が含まれている。

【0065】開始要求メッセージを供給したCPU11は、ステップS4において、通信部24を制御して、開始要求メッセージに対応する応答メッセージである開始応答メッセージを取得したか否かを判定し、取得したと判定するまで待機する。

【0066】開始応答メッセージには、鍵交換方法に関する情報や、使用するアルゴリズムの情報等が含まれており、CPU11は、この開始応答メッセージに基づいて各種の処理を行う。

【0067】通信部24を制御して、開始応答メッセージを取得したと判定した場合、CPU11は、ステップS5に進み、取得した開始応答メッセージに含まれる鍵交換方法に基づいて、鍵生成処理が必要か否かを判定する。鍵生成処理は、通信相手側端末装置4と共有する共通鍵を生成する処理である。必要な場合、CPU11は、ステップS6に進み、通信部24を制御して、鍵交換代行サーバ3に鍵生成処理の代行を要求する鍵生成要求メッセージを供給する。鍵生成要求メッセージを供給したCPU11は、ステップS7において、通信部24を制御して、鍵生成要求メッセージに対応する鍵生成応答メッセージを取得したか否かを判定し、取得するまで待機する。取得したと判定した場合、CPU11は、図5のステップS12に進む。

【0068】また、図4のステップS5において、鍵生

成処理が必要ないと判定した場合、CPU11は、図5のステップS8に進み、開始応答メッセージに含まれる鍵交換方法に基づいて、認証処理が必要か否かを判定する。必要と判定した場合、CPU11は、ステップS9に進み、通信部24を制御して、鍵交換代行サーバ3に、通信相手側端末装置4を認証する認証処理の代行を要求する認証要求メッセージを供給する。

【0069】認証処理の代行を要求したCPU11は、ステップS10に進み、通信部24を制御して、認証要求メッセージに対応する認証応答メッセージを取得したか否かを判定し、取得したと判定するまで待機する。そして、取得したと判定した場合、CPU11は、ステップS11に進み、認証応答メッセージを参照して、通信相手側端末装置4が認証されたか否かを判定する。認証されたと判定した場合、CPU11は、ステップS12に進む。

【0070】ステップS12において、CPU11は、以上の処理により、鍵交換処理において必要な情報が全て揃ったか否かを判定し、揃っていないと判定した場合、図4のステップS5に戻り、それ以降の処理を繰り返す。

【0071】全ての情報が揃ったと判定した場合、CPU11は、ステップS13に進み、通信部24を制御して、鍵交換代行サーバ3に、通信相手側端末装置4との暗号通信において使用されるセッションごとの鍵であるセッション鍵を要求する鍵要求メッセージを供給する。鍵要求メッセージを供給したCPU11は、ステップS14において、通信部24を制御して、鍵要求メッセージに対応する鍵応答メッセージを取得したか否かを判定し、取得したと判定するまで待機する。

【0072】取得したと判定した場合、CPU11は、ステップS15に進み、開始応答メッセージに含まれる鍵交換方法において、鍵応答メッセージの内容に基づいてセッション鍵を生成する必要があるか否かを判定する。生成する必要があると判定した場合、CPU11は、ステップS16に進み、鍵応答メッセージに基づいて、セッション鍵を生成し、ステップS17に進む。また、ステップS15において、鍵応答メッセージにセッション鍵が含まれており、セッション鍵を生成する必要があると判定した場合、CPU11は、ステップS17に進む。

【0073】ステップS17において、CPU11は、通信相手側端末装置4と安全に通信するためのセッション鍵を暗号鍵データベース25に設定し、鍵交換代行処理を終了する。

【0074】また、図5のステップS8において、開始応答メッセージに含まれる鍵交換方法に基づいて、認証処理が必要でないと判定した場合、本来ありえない状態であるので、CPU11は、ステップS18において、誤動作しているとして扱う誤動作処理を行い、ステップS19においてエラー処理を行い、鍵交換代行処理を終了

する。

【0075】また、図5のステップS11において、通信相手側端末装置4が認証されなかったと判定した場合、CPU11は、ステップS19に進み、エラー処理を行い、鍵交換代行処理を終了する。

【0076】次に、図8および図9のフローチャートを参照して、上述した端末装置による鍵交換代行処理に対応する鍵交換代行サーバ3による鍵交換代行処理について説明する。また、必要に応じて、図10および図11を参照して説明する。

【0077】端末装置1の鍵交換処理を代行するCPU51は、最初に、ステップS31において、端末装置1との間に安全な通信路が確保されるか否かを判定する。

【0078】確保されないと判定した場合、CPU51は、ステップS32に進み、端末装置1と安全に通信するための鍵をデータベース65に設定し、ステップS33に進む。なお、設定される鍵は、予め決められており、端末装置1と暗号通信ができるように、端末装置1に設定される鍵と対応してある。また、ステップS31において、端末装置1との間に安全な通信路が確保されると判定した場合、CPU51は、ステップS33に進む。

【0079】上述したように、端末装置1と鍵交換代行サーバ3との間に安全な通信路でない場合は、通信内容を暗号化した暗号通信により行われる。

【0080】図10は、端末装置1と鍵交換代行サーバ3との間に安全な通信路である場合の鍵交換代行サーバ3の通信に関する主な処理の流れを示す図である。

【0081】図10において、CPU51には、各種の処理を実行する処理部121、鍵を生成する鍵生成部122、および認証処理を行う認証部123が構成されている。また、データベース65には、認証部123による認証処理に用いられる認証鍵を管理する認証鍵データベース131、および端末装置1にアクセスすることを許可された装置に関する情報が管理されているポリシデータベース132が設けられている。

【0082】安全な通信路を用いて端末装置1に情報を供給する場合、CPU51の処理部121は、通信部64を介して、端末装置1に情報を供給する。例えば、処理部121は、鍵生成部122において生成された鍵を含むメッセージを、通信部64を介して、端末装置1に供給する。また、安全な通信路を用いて端末装置1より情報を取得する場合、CPU51の処理部121は、通信部24を介して、端末装置1より情報を取得する。

【0083】例えば、処理部121は、通信部64を介して端末装置1より取得した証明書等を認証部123に供給する。認証部123は、データベース65の認証鍵データベース131に登録されている認証鍵に基づいて、通信相手側端末装置4の認証を行い、その認証結果を処理部121に供給する。また、処理部121は、デ

ータベース132のポリシデータベース132に登録されている端末装置1のポリシに関する情報に基づいて、通信相手側端末装置4が端末装置1にアクセス可能か否かを判定する。

【0084】すなわち、鍵交換代行サーバ3は、端末装置1と暗号化されていない通常の通信を行う。

【0085】また、図11は、端末装置1と鍵交換代行サーバ3との間に安全な通信路でない場合の鍵交換代行サーバ3の通信に関する主な処理の流れを示す図である。

【0086】図11において、CPU51には、処理部121、鍵生成部122、および認証部123の他に、処理部121と通信部64の間に、情報を暗号化する暗号通信部141が構成されている。また、データベース65には、認証鍵データベース131、ポリシデータベース132、および、暗号鍵を管理する暗号鍵データベース142が設けられている。暗号通信部141は、暗号鍵データベース142に設定されている暗号鍵に基づいて、情報の暗号化を行う。

【0087】すなわち、鍵交換代行サーバ3は、端末装置1との通信において、暗号通信を行う。従って、この場合、ステップS33以降の処理において、端末装置1と鍵交換代行サーバ3の間の通信は、全て暗号化されて行われる。以下の説明において、鍵交換代行サーバ3による暗号化および復号する処理は図11において説明した場合と同様であるので、その説明は省略する。

【0088】図8に戻り、ステップS33において、CPU51は、通信部64を制御して、端末装置1よりメッセージを取得したか否かを判定し、取得したと判定するまで待機する。取得したと判定した場合、CPU51は、ステップS34に進み、取得したメッセージが開始要求メッセージか否かを判定する。取得したメッセージが、図4のステップS3において、端末装置1より供給された開始要求メッセージであると判定した場合、CPU51は、ステップS35に進み、ステップS35において、取得した開始要求メッセージに基づいて、通信相手側端末装置4との鍵交換方法を決定し、それを含む開始応答メッセージを生成する。そして、ステップS36に進み、CPU51は、通信部64を制御して、生成した開始応答メッセージを端末装置1に供給する。

【0089】そして、ステップS37において、CPU51は、鍵交換代行処理を終了するか否かを判定し、終了しない場合は、ステップS33に戻り、それ以降の処理を繰り返す。また、ステップS37において、終了すると判定した場合、CPU51は、鍵交換代行処理を終了する。

【0090】図8のステップS34において、取得したメッセージは開始要求メッセージではないと判定した場合、CPU51は、ステップS38に進む。ステップS38において、CPU51は、取得したメッセージが鍵生成

10

20

30

40

50

要求メッセージか否かを判定する。鍵生成要求メッセージであると判定した場合、CPU5 1は、ステップS39に進み、鍵生成要求メッセージに基づいて、鍵を生成する。そして、ステップS40において、CPU5 1は、生成した鍵を含む鍵生成応答メッセージを、通信部64を介して端末装置1に供給する。端末装置1に鍵生成応答メッセージを供給したCPU5 1は、ステップS37に戻り、それ以降の処理を繰り返す。

【0091】また、図8のステップS38において、取得したメッセージは鍵生成要求メッセージではないと判定した場合、CPU5 1は、図9のステップS41に進む。図9のステップS41において、CPU5 1は、取得したメッセージが認証要求メッセージであるか否かを判定する。認証要求メッセージであると判定した場合、CPU5 1は、ステップS42に進み、図10のデータベース65の認証鍵データベース131に保持されている認証鍵を利用して認証処理を行う。そして、ステップS43において、CPU5 1は、ポリシーデータベース43により保持されているポリシーを確認し、通信相手側端末装置による端末装置へのアクセスが許可されているか否かを
20 確認する処理を行い、ステップS44において、認証結果および確認結果を含む認証応答メッセージを、通信部64を制御して、端末装置1に供給する。端末装置1に認証応答メッセージを供給したCPU5 1は、ステップS37に戻り、それ以降の処理を繰り返す。

【0092】ステップS41において、取得したメッセージが認証要求メッセージではないと判定した場合、CPU5 1は、ステップS45に進み、取得したメッセージが鍵要求メッセージか否かを判定する。鍵要求メッセージであると判定した場合、CPU5 1は、ステップS46
30 に進み、図8のステップS35において決定した鍵交換方法に基づいて、セッション鍵を生成する必要があるか否かを判定する。そして、必要があると判定した場合、CPU5 1は、ステップS47に進み、通信相手側端末装置4との通信に利用するセッション鍵を生成し、ステップS48に進む。また、生成する必要があると判定した場合、CPU5 1は、ステップS48に進む。そして、ステップS48において、CPU5 1は、上述した処理の結果を踏まえた鍵応答メッセージを生成し、通信部64を
40 制御して、端末装置1に供給する。鍵応答メッセージを端末装置1に供給したCPU5 1は、ステップS37に戻り、それ以降の処理を繰り返す。

【0093】また、ステップS45において、取得したメッセージが鍵要求メッセージではないと判定した場合、CPU5 1は、ステップS49において、この不明なメッセージを破棄し、ステップS37に戻り、それ以降の処理を繰り返す。

【0094】以上のように、端末装置1および鍵交換代行サーバ3において鍵交換代行処理を行うことにより、
50 鍵交換処理における端末装置1の負担を軽減することが

できる。

【0095】次に、図12乃至図14を参照して、上述した鍵交換処理代行システムの既存の鍵交換処理への適用例を説明する。

【0096】図12は、本発明を適用した鍵交換処理代行システムのIKEへの適用例を示す図である。図12においては、端末装置1が通信相手側端末装置4とIKEにより鍵交換を行う際に、鍵交換代行サーバ3により、
端末装置1が行うPhase1の鍵交換処理の一部を代行して
いる。

【0097】最初に、ステップS101において、通信相手側端末装置4が通信を保護するために用いられる方針や鍵の集合からなる情報を含むSAベイロードを端末装置1に供給し、端末装置1は、ステップS121において、そのSAベイロードを取得する。

【0098】SAベイロードを受信すると端末装置1は、ステップS122で、SAベイロードや利用可能な暗号化アルゴリズム等を含む開始要求メッセージを鍵交換代行サーバ3に供給する。この処理は、図4のステップS3
の処理に対応する。鍵交換代行サーバ3は、ステップS151において、端末装置1より供給された開始要求メッセージを取得すると、決定した鍵交換方法等の情報を含む返信用のSAベイロードを生成し、その返信用SAベイロードを含む開始応答メッセージを生成して端末装置1
に供給する。この処理は、図8のステップS34乃至ステップS36の処理に対応する。

【0099】鍵交換代行サーバ3より供給された開始応答メッセージは、端末装置1によりステップS123において取得される。この処理は、図4のステップS4の
処理に対応する。そして、開始応答メッセージを取得した端末装置1は、ステップS124において、開始応答メッセージに含まれる返信用のSAベイロードを通信相手
側端末装置4にIKEのSAベイロードとして供給する。

【0100】通信相手側端末装置4は、ステップS102において、そのSAベイロードを取得すると、ステップS103において、共有秘密として使用される鍵情報を含む鍵交換ベイロード、および、乱数情報を含むNonce
ベイロードを端末装置1に供給する。端末装置1は、ステップS125において、その鍵交換ベイロードおよび
Nonceベイロードを取得する。端末装置1は、ステップS126において、取得した鍵交換ベイロードを含む鍵
生成要求メッセージを鍵交換代行サーバ3に供給する。この処理は、図4のステップS6の処理に対応する。鍵
交換代行サーバ3は、ステップS153において、端末
装置1より供給された鍵生成要求メッセージを取得すると、返信用の鍵交換ベイロードを生成し、ステップS1
54において、作成した返信用の鍵交換ベイロードを含
む鍵生成応答メッセージを端末装置1に供給する。ま
た、鍵交換ベイロードの内容に基づいて、ISAKMP SAを
生成する。これらの処理は、図8のステップS38乃至

ステップS40の処理に対応する。

【0101】端末装置1は、ステップS127において鍵生成応答メッセージを取得する。この処理は図4のステップS7の処理に対応する。端末装置1は、ステップS128において、鍵生成応答メッセージに含まれる返信用の鍵交換ペイロードおよびNonceペイロードを通信相手側端末装置4に供給する。通信相手側端末装置4は、この返信用の鍵交換ペイロードおよびNonceペイロードをステップS104において取得すると、ステップS105において、IDペイロードおよび署名ペイロードを端末装置1に供給する。

【0102】端末装置1は、ステップS129において、IDペイロードおよび署名ペイロードを取得すると、ステップS130において、署名ペイロードを含む認証要求メッセージを鍵交換代行サーバ3に供給する。この処理は、図5のステップS9の処理に対応する。ステップS155において、鍵交換代行サーバ3は、端末装置1より供給された認証要求メッセージを取得すると、認証要求メッセージに含まれる署名に基づいて認証処理を行い、認証されると返信用の署名ペイロードを生成し、ステップS156において、生成した返信用の署名ペイロードを含む認証応答メッセージを端末装置1に供給する。この処理は、図9のステップS41乃至ステップS44の処理に対応する。

【0103】ステップS131において、端末装置1は、鍵交換代行サーバ3より供給された認証応答メッセージを取得する。この処理は、図5のステップS10の処理に対応する。端末装置1は、ステップS132においてIDペイロードおよび署名ペイロードを通信相手側端末装置4に供給する。通信相手側端末装置4は、そのIDペイロードおよび署名ペイロードを、ステップS106において、取得する。

【0104】また、端末装置1は、ステップS133において、鍵交換代行サーバ3に鍵要求メッセージを供給する。この処理は、図5のステップS13の処理に対応する。鍵交換代行サーバ3は、ステップS157において、端末装置1より鍵要求メッセージを取得すると、セッション鍵を生成し、ステップS158において、端末装置1に鍵応答メッセージを供給する。この処理は、図9のステップS45乃至ステップS48の処理に対応する。そして、端末装置1は、鍵交換代行サーバ3より供給された鍵応答メッセージをステップS134において取得する。この処理は、図5のステップS14の処理に対応する。

【0105】端末装置1は、鍵応答メッセージに含まれるISAKMP SAを設定し、Phase2の通信に利用する。

【0106】図13は、図12に示した処理に続いて行われるPhase2の処理の例を示す図である。Phase2においては、認証に関連する情報のみが交換される。

【0107】図13において、通信相手側端末装置4

は、ステップS171において、その状況下でトラフィックを保護するのに適していると考えられるProposalを生成し、ハッシュペイロード、SAペイロード、およびNonceペイロードを端末装置1に供給する。端末装置1は、ステップS191において、これらのハッシュペイロード、SAペイロード、およびNonceペイロードを取得する。

【0108】そして、端末装置1は、ステップS192において、それが受け入れる保護スートを指示するために、返信用のハッシュペイロード、SAペイロード、およびNonceペイロードを通信相手側端末装置4に供給する。通信相手側端末装置4は、これらの返信用のハッシュペイロード、SAペイロード、およびNonceペイロードを、ステップS172において、取得する。

【0109】最後に、通信相手側端末装置4は、ステップS173において、ハッシュペイロードを端末装置1に供給し、端末装置1は、そのハッシュペイロードをステップS193において取得する。

【0110】以上のように、本発明を適用した鍵交換処理代行システムは、IKEによる鍵交換に適用される。

【0111】図14は、本発明を適用した鍵交換処理代行システムのTLS Handshake Protocolへの適用例を示す図である。図14においては、端末装置1が通信相手側端末装置4とTLS Handshake Protocolにより鍵交換を行う際に、鍵交換代行サーバ3により、端末装置1が行う鍵交換処理の一部を代行している。このとき、端末装置1がTLSクライアントとなり、通信相手側端末装置4がTLSサーバとなっている。

【0112】最初に、端末装置1は、ステップS331において、利用可能な暗号化アルゴリズム等を含めた開始要求メッセージを鍵交換代行サーバ3に供給する。この処理は、図4のステップS3の処理に対応する。鍵交換代行サーバ3は、ステップS351において、この開始要求メッセージを取得すると、開始要求メッセージに含まれている暗号化アルゴリズム等と、鍵交換代行サーバ3において利用可能な暗号化アルゴリズム等とから、TLS Handshake Protocolで利用するアルゴリズムを決定し、開始応答メッセージに含めて端末装置1に供給する。これらの処理は、図8のステップS34乃至ステップS36の処理に対応する。

【0113】端末装置1は、ステップS322において、鍵交換代行サーバ3より供給された開始応答メッセージを取得する。この処理は、図4のステップS4の処理に対応する。開始応答メッセージを取得した端末装置1は、ステップS323において、開始応答メッセージの内容に基づいて、TLS Handshake ProtocolのClientHelloメッセージを生成し、通信相手側端末装置4に供給する。通信相手側端末装置4は、このClientHelloメッセージをステップS301において取得すると、ステップS302において、ServerHelloメッセージを端末装

置1に供給し、Certificateメッセージを端末装置1に供給し、ServerHelloDoneメッセージを端末装置1に供給する。端末装置1は、それらのメッセージを、ステップS324において取得する。

【0114】Certificateメッセージを取得した端末装置1は、ステップS325において、取得したCertificateメッセージを含めた認証要求メッセージを鍵交換代行サーバ3に供給する。この処理は、図5のステップS9の処理に対応する。鍵交換代行サーバ3は、ステップS353において、この認証要求メッセージを取得し、10 認証要求メッセージに含まれるTLS Handshake ProtocolのCertificateメッセージに基づいて、通信相手側端末装置4を認証し、ステップS354において、認証結果を含めた認証応答メッセージを端末装置1に供給する。これらの処理は、図9のステップS41乃至ステップS44の処理に対応する。

【0115】ステップS326において、端末装置1は、認証応答メッセージを取得する。この処理は、図5のステップS10の処理に対応する。端末装置1は、ステップS327において、pre-master keyを生成するた20 ために、鍵生成要求メッセージを鍵交換代行サーバ3に供給する。鍵交換代行サーバ3は、ステップS355において、鍵生成要求メッセージを取得すると、取得した鍵生成応答メッセージの内容に基づいて、TLS Handshake ProtocolのClient Key Exchangeメッセージに必要な情報を算出し、ステップS356において、その情報を含めた鍵生成応答メッセージを端末装置1に供給する。これらの処理は、図8のステップS38乃至ステップS40の処理に対応する。

【0116】鍵交換代行サーバ3より供給された鍵生成30 応答メッセージは、ステップS328において、端末装置1により取得される。この処理は、図4のステップS7の処理に対応する。端末装置1は、取得した鍵生成応答メッセージの内容に基づいて、TLS Handshake ProtocolのClient Key Exchangeメッセージを生成し、ステップS329において、生成したClient Key Exchangeメッセージを通信相手側端末装置4に供給する。通信相手側端末装置4は、このClient Key Exchangeメッセージを、ステップS303において取得する。

【0117】端末装置1は、ステップS330において、さらに、TLS Record Protocolで利用されるpre-master keyから生成される各種鍵情報を要求するための鍵40 要求メッセージを鍵交換代行サーバ3に送信する。この処理は、図5のステップS13の処理に対応する。鍵交換代行サーバ3は、ステップS357において、この鍵要求メッセージを取得し、pre-master keyからTLS Record Protocolで利用するセッション鍵を生成し、ステップS358において、生成したセッション鍵を含む鍵応答メッセージを端末装置1に供給する。これらの処理は、図9のステップS45乃至ステップS48の処理に

対応する。

【0118】端末装置1は、ステップS331において、鍵交換代行サーバ3に供給された鍵応答メッセージを取得し、取得した鍵応答メッセージの内容に基づいて、TLS Record Protocolで利用するセッション鍵を設定する。これらの処理は、図5のステップS15乃至ステップS17の処理に対応する。

【0119】以上のように、本発明を適用した鍵交換処理代行システムは、TLS Handshake Protocolによる鍵交換に適用される。

【0120】一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【0121】この記録媒体は、図2および図3に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク41および81（フロッピーディスクを含む）、光ディスク42および82（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク43および83（MD(Mini-Disc)を含む）、もしくは半導体メモリ44および84などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているCPU11および51に内蔵されているROMなどで構成される。

【0122】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0123】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0124】

【発明の効果】以上のように、本発明のネットワークシステムによれば、通信を行う情報処理装置の鍵交換処理による負担を軽減することができ、計算資源が限られた機器においても、既存の鍵交換プロトコルとの互換性を保ちつつ鍵交換を実現することができる。

【0125】本発明の第1の情報処理装置および方法、記録媒体、並びにプログラムによれば、鍵交換処理による負担を軽減することができ、計算資源が限られた機器である場合も、既存の鍵交換プロトコルとの互換性を保ちつつ鍵交換を実現することができる。

【0126】本発明の第2の情報処理装置および方法、記録媒体、並びにプログラムによれば、通信を行う情報

処理装置の鍵交換処理による負担を軽減することができ、計算資源が限られた機器においても、既存の鍵交換プロトコルとの互換性を保ちつつ鍵交換を実現することができる。

【図面の簡単な説明】

【図1】本発明を適用した鍵交換処理代行システムの構成例を表している。

【図2】図1の端末装置の構成例を示すブロック図である。

【図3】図1の鍵交換代行サーバの構成例を示すブロック図である。

【図4】端末装置による鍵交換代行処理を説明するフローチャートである。

【図5】端末装置による鍵交換代行処理を説明する、図4に続くフローチャートである。

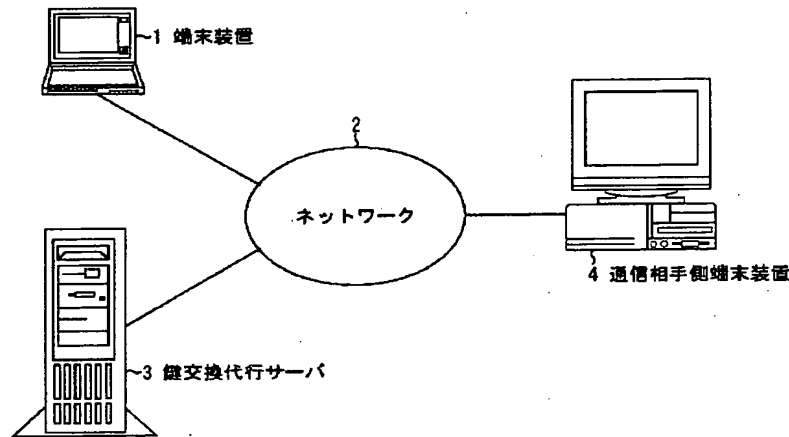
【図6】端末装置と鍵交換代行サーバとの間が安全な通信路である場合の、端末装置の通信に関する主な処理の流れを示す図である。

【図7】端末装置と鍵交換代行サーバとの間が安全な通信路でない場合の、端末装置の通信に関する主な処理の流れを示す図である。

【図8】鍵交換代行サーバによる鍵交換代行処理について説明するフローチャートである。

【図9】鍵交換代行サーバによる鍵交換代行処理について説明する、図8に続くフローチャートである。

【図1】



*【図10】端末装置と鍵交換代行サーバとの間が安全な通信路である場合の、鍵交換代行サーバの通信に関する主な処理の流れを示す図である。

【図11】端末装置と鍵交換代行サーバとの間が安全な通信路でない場合の、鍵交換代行サーバの通信に関する主な処理の流れを示す図である。

【図12】本発明を適用した鍵交換処理代行システムのIKEへの適用方法の例を説明するフローチャートである。

【図13】図12の処理に続く処理の例を説明するフローチャートである。

【図14】本発明を適用した鍵交換処理代行システムのTLS Handshake Protocolへの適用方法の例を説明するフローチャートである。

【符号の説明】

1 端末装置, 2 ネットワーク, 3 鍵交換代行サーバ, 4 通信相手側端末装置, 11 CPU, 12 ROM, 13 RAM, 23 記憶部, 24 通信部, 25 暗号鍵データベース, 51 CPU, 52 ROM, 53 RAM, 63 記憶部, 64 通信部, 65 データベース, 101 処理部, 102 暗号通信部, 121 処理部, 122 鍵生成部, 123 認証部, 131 認証鍵データベース, 132 ポリシデータベース, 141 暗号通信部, 142 暗号鍵データベース

【図2】

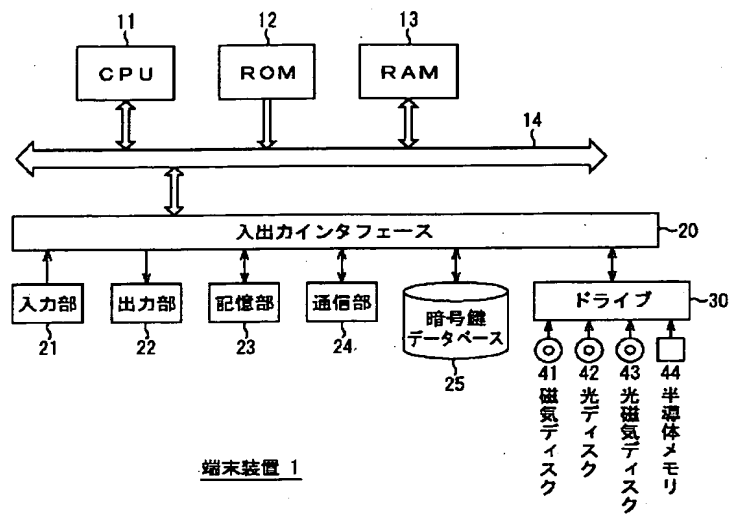


図2

【図3】

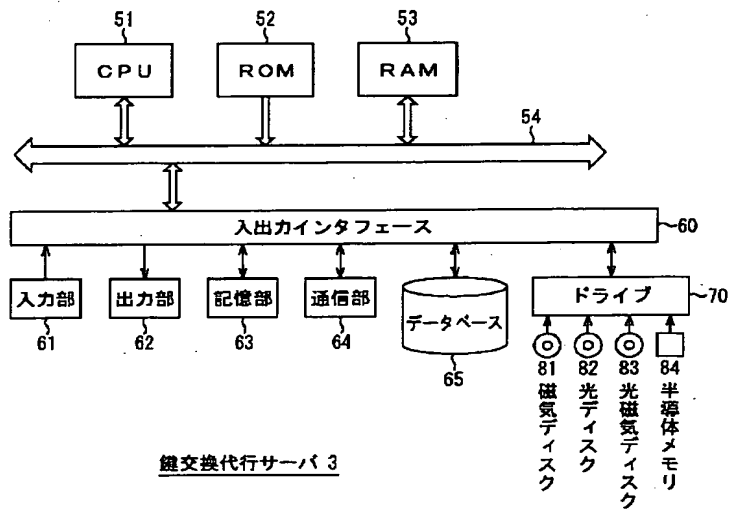
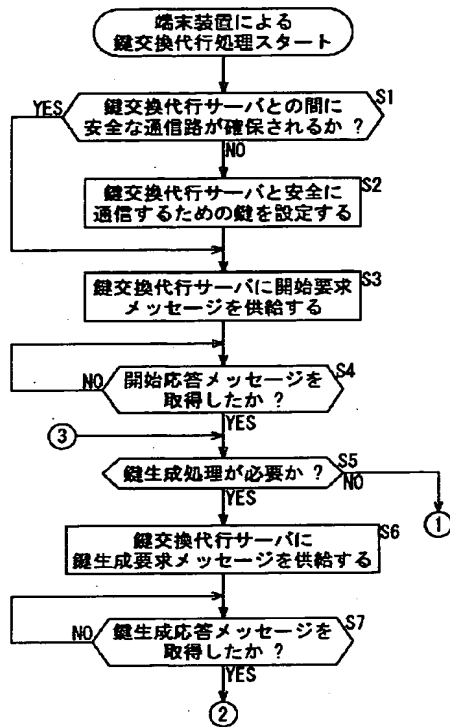


図3

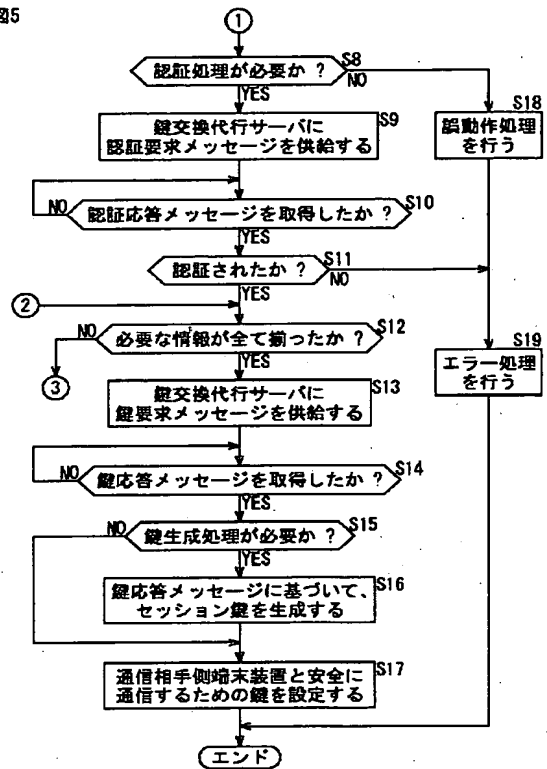
【図4】

図4



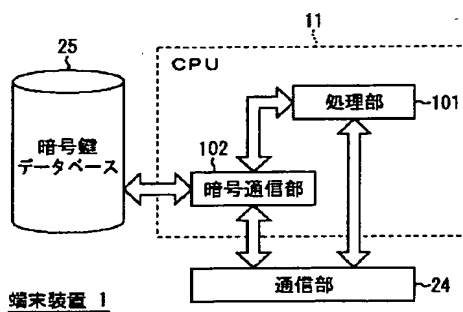
【図5】

図5



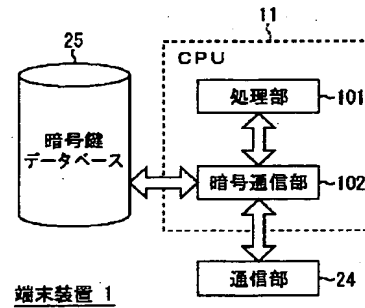
【図6】

図6

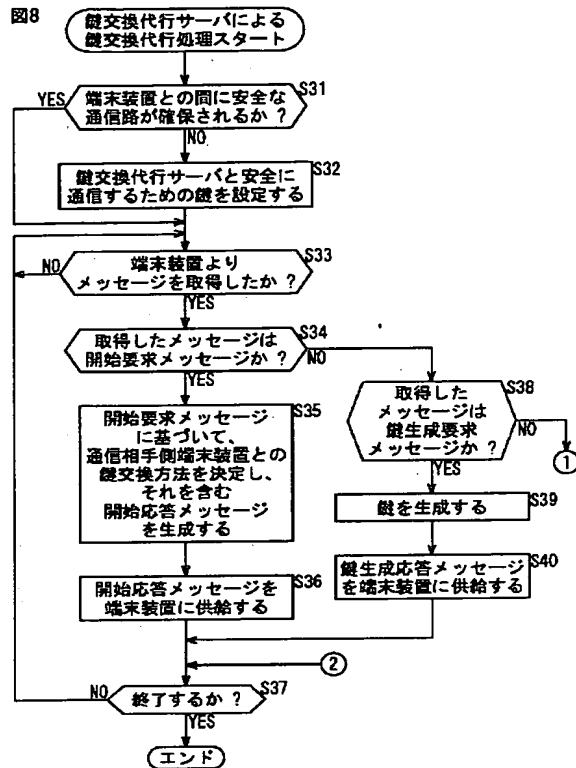


【図7】

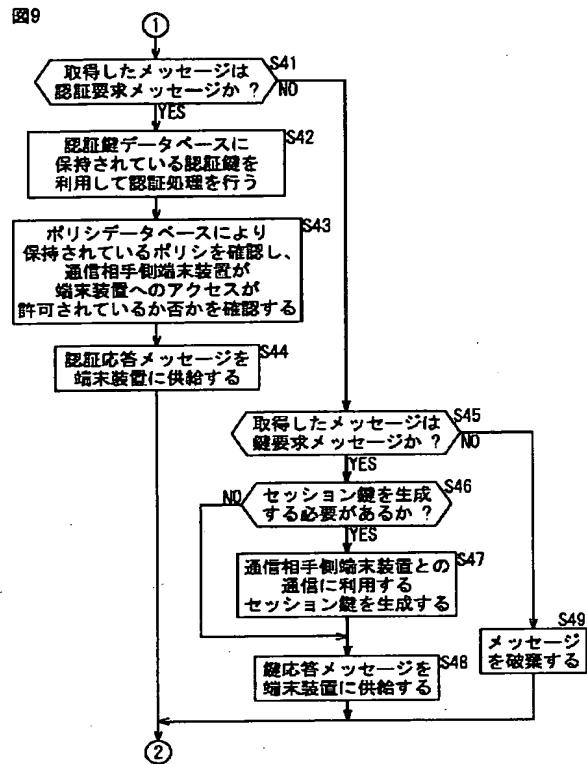
図7



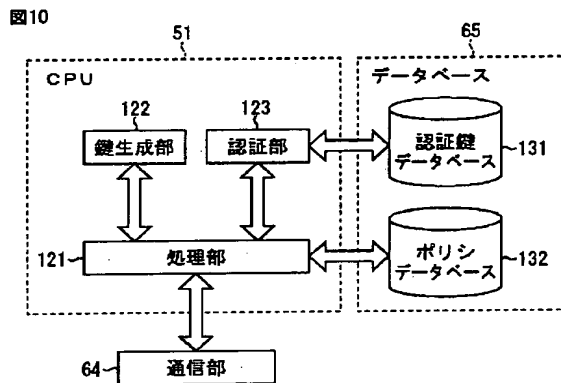
【図8】



【図9】

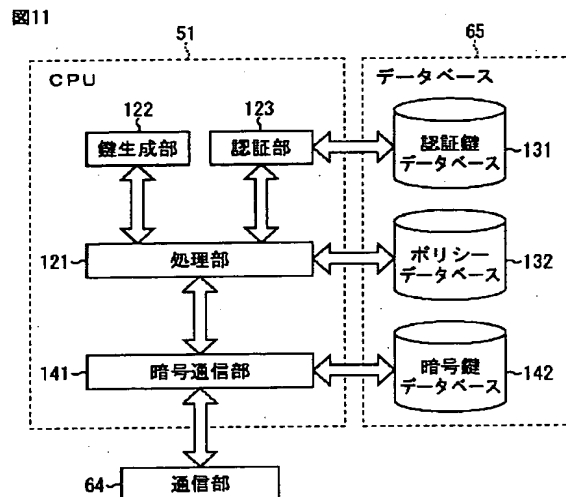


【図10】



鍵交換代行サーバ 3

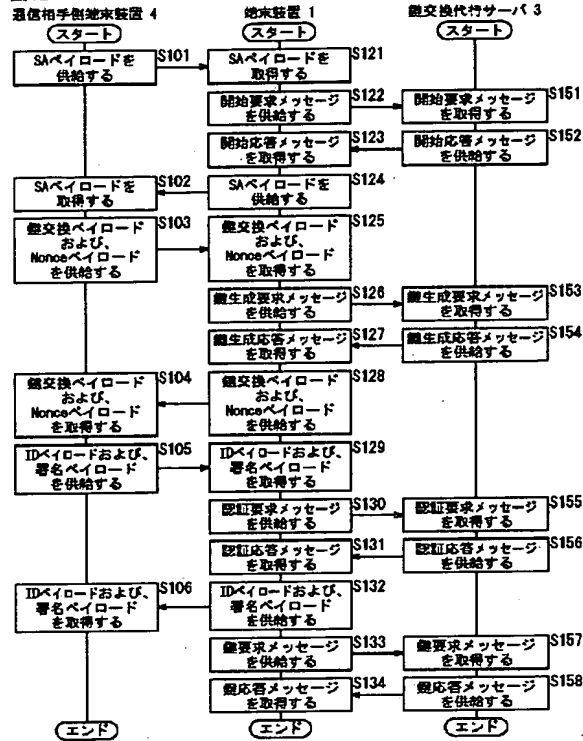
【図11】



鍵交換代行サーバ 3

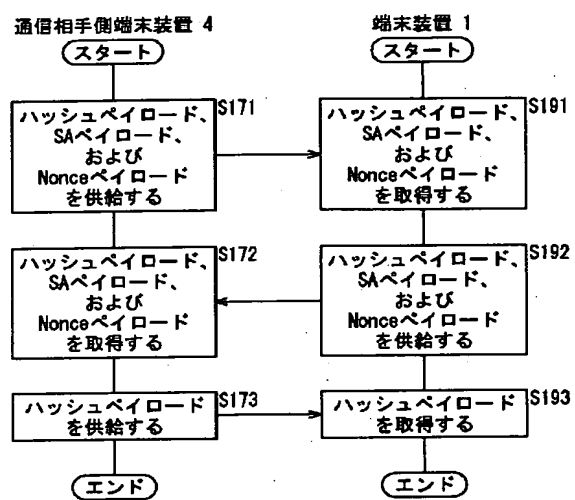
【図12】

図12



【図13】

図13



【図14】

図14

